

1 **ABSTRACT**

2 Packet filters and network virtualization are used to restrict network
3 communications. A network mediator corresponding to a computing device uses
4 packet filters to restrict network communications. The network mediator includes
5 a set of one or more filters, each filter having parameters that are compared to
6 corresponding parameters of a data packet to be passed through the network
7 mediator (either from or to the computing device). The network mediator
8 determines whether to allow the data packet through based on whether the data
9 packet parameters match any filter parameters. The set of filters can be modified
10 by a remote device, but cannot be modified by the computing device whose
11 communications are being restricted (thereby preventing the device whose
12 communications are being restricted from being able to modify those restrictions).
13 Additionally, the set of filters may be modified by remote devices at different
14 managerial levels, although remote devices are prohibited from modifying filters
15 to make the filters less restrictive than filters imposed by higher level devices.
16 Network virtualization can be also be used, either in addition to or in combination
17 with the packet filters, to restrict network communications by the network
18 mediator maintaining a mapping of virtual addresses to network addresses, and
19 allowing the computing device to access only the virtual addresses. When a data
20 packet is sent from the computing device, the data packet will include the virtual
21 address which is changed to the network address by the network mediator prior to
22 forwarding the packet on the network. Similarly, when a data packet is received at
23 the network mediator targeting the computing device, the network mediator
24 changes the network address in the data packet to the corresponding virtual
25 address. By virtualizing the addresses, the computing device is restricted in its

